



DEPARTMENT OF THE ARMY
UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
UNIT 29351
APO AE 09014-9351

AEAIM-A

2 September 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Wireless Information Systems and Wireless Portable Electronic Devices

This memorandum expires in 1 year.

1. This memorandum supersedes memorandum, HQ USAREUR/7A, AEAIM-A, 17 March 2004, subject as above.

2. References:

a. "Wireless Security Technical Implementation Guide (STIG)," Defense Information Systems Agency, 7 April 2004 (available at <https://iase.disa.mil/documentlib.html#wirelessguid>).

b. "Wireless Security Checklist," Defense Information Systems Agency, 30 July 2003 (available at <http://csrc.nist.gov/pcig/CHECKLISTS/wireless-chklstv2r11-073003.doc>).

c. DOD Directive 5000.1, The Defense Acquisition System, 12 May 2003.

d. DOD Direction 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004.

e. DOD C-5105.21-M-1, Sensitive Compartmented Information (SCI) Security Manual Administrative Security, March 1995.

f. AR 5-12, Army Management of the Electromagnetic Spectrum, 20 December 1994.

g. AR 25-1, Army Knowledge Management and Information Technology Management, 30 June 2004.

h. AR 25-2, Information Assurance, 4 November 2003.

3. Wireless information systems (IS) are wireless telecommunications or computer-related equipment or interconnected systems or subsystems of equipment (including software, firmware, and hardware) used to support Army business, operations, and missions in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice or data. Wireless IS include cell phones, personal communications system (PCS) devices, Blackberry devices, and use of Bluetooth technology; this does not include one-way, receive-only devices.

4. This policy applies to all Army in Europe organizations and DOD organizations that use Army in Europe LandWarNet (Unclas) networks.

5. In addition to the general security regulations and policy in the references, wireless IS will be controlled as follows in the European theater:

This memorandum is available at <https://www.aeaim.hqusareur.army.mil/library/>.

AEAIM-A

SUBJECT: Wireless Information Systems and Wireless Portable Electronic Devices

a. Requests to implement a wireless solution must be sent to the USAREUR G6 (AEAIM-C) for evaluation and approval. Each request must support an operational and mission need that cannot be met without the use of the wireless IS.

b. Pilot and fielded wireless local area networks (LANs) and portable electronic devices (PEDs) with LAN connectivity must meet the same certification and accreditation (C&A) and information assurance (IA) requirements as wired LAN IS (AR 25-1 and AR 25-2) within 6 months from the date of this policy.

c. The reference in paragraph 2a (commonly referred to as the STIG) will be used to help improve the security of DOD wireless IS. Wireless devices and systems that do not meet the security requirements of the STIG or of other appropriate DOD or Army policy will not be used to store, process, or transmit DOD information on AE networks unless approved by the designated accreditation authority (DAA) as necessary to meet specific mission requirements. The reference in paragraph 2b must also be used to help confirm compliance with the requirements of the STIG and other policy guidance.

d. Wireless IS will not be configured to work with any device other than a Government-owned computer. When an approved device is used outside of the Army's infrastructure (for example, during temporary duty (TDY)), the device must be scanned for malicious codes before being reconnected to the AE backbone.

e. The USAREUR G6 (AEAIM-C/Frequency Management Branch) will certify that the device complies with spectrum supportability standards. All wireless devices must meet spectrum supportability and comply with Military Communications-Electronics Board (MCEB) standards, DOD Directive 5000.1, AR 5-12, and host-nation requirements. Because wireless devices do not require frequency assignments, the user will accept any interference received.

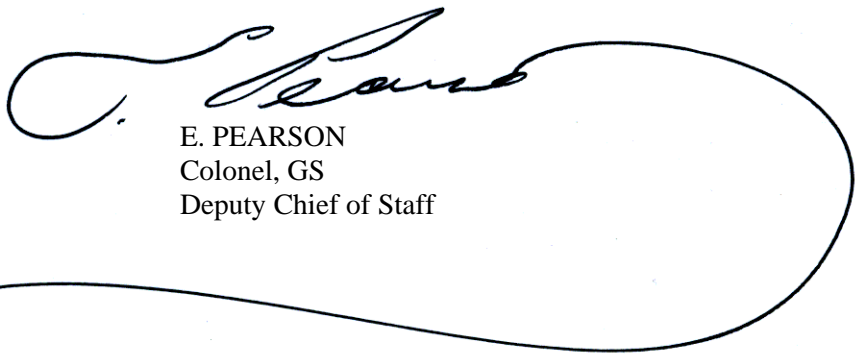
6. POCs are—

a. For technical information: Mr. Meyer, DSN 370-7151, e-mail: james.meyer@us.army.mil.

b. For frequency management: Master Sergeant Figueroa, DSN 370-3095, e-mail: freddy.figueroa@us.army.mil.

c. For policy: Ms. Holland, DSN 370-3520, e-mail: karen.holland@us.army.mil.

FOR THE COMMANDER:



E. PEARSON
Colonel, GS
Deputy Chief of Staff

DISTRIBUTION:
C (AEPUBS)